הנחית רשם מאגרי מידע מס' 2/2011

שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי

1. מטרה

1.1. העזרות בשירותי מיקור חוץ (outsourcing) מהווה מרכיב משמעותי בפעילותם של ארגונים במשק מודרני. במקרים רבים, שירותי מיקור החוץ כרוכים בניהול מידע אישי המעובד בארגון באופן ממוחשב.

1.2. מטרת הנחיה זו היא להבהיר את עמדתו של רשם מאגרי המידע בדבר הפעולות הראויות לקיום חובותיהם של בעל מאגר המידע, מנהל מאגר המידע והמחזיק בו לגבי עיבוד מידע אישי אגב מיקור חוץ מכוח הוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן - **החוק**) והתקנות לפיו[1].

1.3. יובהר, כי נוסף על הנחיה זו, בעת שימוש בשירות מיקור החוץ הכולל גם העברת מידע אישי אל מחוץ לגבולות ישראל, יש לוודא קיום הוראות תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001[2].

2. רקע

2.1. השימוש בשירותי מיקור חוץ משמעו הוצאה מחוץ לארגון, או ביצוע על ידי מי שאינם עובדי ארגון, של פעולות ותהליכים המבוצעים בדרך כלל על ידי הארגון, במטרה לקדם יעילות, להוזיל עלויות ולהתמקד בליבת העיסוק של הארגון.

2.2. כתוצאה מכך נדרשת הסדרה משפטית וארגונית כדי להבטיח מימוש יעדי הארגון בביצוע השירות, שלא באמצעות עובדיו. במסגרת זו נדרשת מניעת הסיכונים הנובעים מכך שהשירות מבוצע במיקור חוץ[3].

---

[1] במחלקת יעוץ וחקיקה במשרד המשפטים נמצאת בשלבים מתקדמים הכנה של הנחיית יועץ משפטי לממשלה בנושא מיקור חוץ בידי גופים ציבורים. ככל שיידרש, הנחייה זו תתוקן לאחר פרסום הנחיית היועץ.

[2] בכוונת הרשם לפרסם הנחיה אשר תעסוק בנושא השימוש בשירותי "מחשוב ענן" (cloud computing), שתהיה משלימה להנחיה זו.

[3] בגוף ציבורי נדרשת בחינה של עצם ההחלטה על שימוש במיקור חוץ, בשים לב למספר היבטים ייחודיים לגופים אלה: הדינים החלים על הגוף הציבורי, היקף המידע המוחזק על ידו והיות איסוף המידע מכוח סמכות חוקית לעומת על בסיס הסכמה של האזרח נושא המידע.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

2.3. חוק הגנת הפרטיות ובפרט העקרונות הקבועים בפרק ב' בו, מסדיר את השימוש החוקי במידע אודות אדם כהגדרתו בחוק וקובע את מסגרות ההגנה כנגד שימוש לרעה באותו מידע. על מנת להשיג תכלית זו, מטיל פרק ב' בחוק אחריות למניעת שימוש לרעה במידע, דליפה או גניבה של המידע על מי שאוסף ומעבד מידע עבור עצמו ועל מי שמספק לו שירותים.

2.4. בשירותי מיקור חוץ יש חשיבות רבה לרמת רגישות המידע המוצא למיקור חוץ. בחינת רמת הרגישות של המידע נגזרת הן מפרמטרים כמותיים (כגון מספר נושאי המידע, היקף המידע, מספר בעלי הרשאת הגישה למידע), והן מפרמטרים מהותיים (כגון סוג המידע).

2.5. בעת השימוש בשירותי מיקור חוץ החובות והאחריות המוטלים מכוח החוק על בעל מאגר מידע, מנהל מאגר מידע והמחזיק בו ממשיכים לחול על כל אחד מהם כאילו הוא מבצע את הפעילות בעצמו, כולל, בין היתר, עקרון "הגבלת המטרה" לפי הוראות פרקים ב' ו-ד' לחוק הגנת הפרטיות, ובמיוחד בסעיפים 2(9) ו- 8(ב) לחוק, חובת אבטחת המידע והבטחת מימוש זכויות נושא המידע.

3. הנחיה

3.1. לאור האמור לעיל, עמדת רשם מאגרי המידע בדבר הפעולות הראויות לקיום חובותיהם של בעל מאגר המידע, מנהל מאגר המידע והמחזיק בו לגבי עיבוד מידע אישי אגב מיקור חוץ מכוח הוראות החוק והתקנות שמכוחו הינה כדלקמן:

3.1.1. <u>הוצאת פעילות למיקור חוץ – בדיקה מקדמית, היקף ומודל אספקת שירות</u>

3.1.1.1. על ארגון המבקש להוציא פעילות למיקור חוץ (להלן - **המזמין**) לבחון **האם הוא רשאי להוציא את המידע שהוא מבקש לעבד במיקור חוץ אל מחוץ לשליטתו בתהליך של מיקור חוץ**, שכן עשויות להיות מגבלות חוקיות או אתיות, אשר מונעות העברה כאמור. אף אם אין מגבלה פורמלית כאמור, מומלץ לקיים הליך בחינה האם ראוי, לאור אופי המידע האישי שהשירות יתבקש לגביו ורגישותו, להעביר את המידע או את העיבוד שלו למיקור חוץ.

3.1.1.2. על המזמין **להגדיר בפירוט מהו סוג השירות המבוקש על ידו, וכפועל יוצא מכך - מהו היקף המידע האישי הנדרש לצורך אספקת השירות על ידי נותן שירות מיקור החוץ (להלן - הקבלן)**. הגדרה זאת ראוי שתיכלל במסגרת אפיון כולל של השירות המבוקש המוצג בשלב ההזמנה להציע הצעות או כנספח למכרז או לחוזה. לעניין זה קיימים שלושה מודלים:

3.1.1.2.1. שירות המחייב טיפול במידע אישי החל משלב איסוף המידע מנושאי המידע בשם המזמין ועיבוד המידע על ידי הקבלן, לרבות ההקמה מאגר המידע;

3.1.1.2.2. שירות המחייב העברה או העתקה של מאגר מידע שלם, או חלק מהותי ממנו, מהמזמין לקבלן;

3.1.1.2.3. שירות המחייב טיפול במידע אישי בדרך של מתן הרשאות גישה או עדכון למידע במאגר המידע אצל המזמין, בהיקף הנדרש לצורך מתן שירות ספציפי, ללא העברת מאגר המידע במלואו.

כנקודת מוצא יש להעדיף את חלופה 3.1.1.2.3 לעיל, שכן העברת עותק שלם של מאגר מידע לקבלן או מתן גישה בלתי-מוגבלת למערכות המזמין, מציבים סיכון ממשי של העברת מידע עודף, שאינו דרוש במישרין למילוי תפקידו החוזי של הקבלן. בנוסף, בחלופות 3.1.1.2.1 ו-3.1.1.2.2 מאבד המזמין את יכולת השליטה בשימוש במאגר המידע. למעלה מכך, הניסיון מלמד כי הרשאות גישה נדיבות מדי מזמנות סיכוני אבטחת מידע שניתן להימנע מהם. **בחירה בחלופה 3.1.1.2.3 לעיל, יחד עם שימוש באמצעים אשר יבטיחו הגבלה של מתן הרשאות גישה למידע ובקרה על שימושים חריגים בהרשאות, יצמצמו במידה ניכרת את הסיכונים הנובעים מעיבוד מידע. כתוצאה מכך ניתן יהיה להקל בדרישות הקשורות בהסדרת נושא זה במסגרת התפעול והפיקוח השוטפים**. ככל שנבחרת חלופה אחרת, יש לתעד את ההצדקה לבחירה בחלופה זו נוכח הנאמר לעיל.

3.1.2. <u>בחירת הקבלן</u>

3.1.2.1. **בבחירת הקבלן המבצע את מיקור החוץ על המזמין לבחון את ההיבטים הבאים**:

3.1.2.1.1. ניסיון קודם של הקבלן בעיבוד מידע אישי;

3.1.2.1.2. רקע ומוניטין של הקבלן;

3.1.2.1.3. קיום חשש לניגוד עניינים מובנה או סיכון אחר לשימוש פסול במידע על ידי הקבלן או מי מטעמו.

3.1.2.2. ככל שהמידע המועבר לקבלן הוא רגיש יותר, כך יש לנקוט במשנה זהירות בבחירת הקבלן.

3.1.3. <u>ניסוח חוזה ההתקשרות</u>

3.1.3.1. **צמידות מטרה** - על המזמין **להגדיר מפורשות את המטרות המותרות לשימוש ואת סוג בעלי התפקידים המועסקים על ידי הקבלן שיהיו מורשים בגישה אל המידע, וזאת על מנת להקפיד שהקבלן** ישתמש במידע אך ורק לשם ביצוע המטרה המקורית של הפעילות שביצועה הועבר אליו. יש לוודא שהחוזה מנוסח בבהירות הן בהגדרת המטרה והן בדרכים למימוש מטרה זו. יש לדרוש כי הקבלן ידריך את עובדיו במטרות השימוש במידע, ויוכיח את קיום ההדרכות למזמין.

3.1.3.2. **במקרה בו הקבלן אוסף מידע ישירות מנושא המידע, על המזמין לוודא כי הקבלן יקיים ויקפיד הקפדה יתירה על קיום חובת ההודעה הקבועה בסעיף 11 לחוק**. נוסח ההודעה ואופן קיומה צריכים להיקבע על ידי המזמין, או להיות מאושרים על ידו.

3.1.3.3. **על המזמין לאסור במפורש על הקבלן לאסוף מידע בדרכים בלתי-חוקיות, או לעשות שימוש במאגרי מידע בלתי-חוקיים**.

3.1.3.4. **על חוזה ההתקשרות עם הקבלן להכיל בטוחות, לרבות חיוב עריכת ביטוח אחריות מקצועית, סעדים וכלי בקרה אפקטיביים שיאפשרו תגובה מהירה ויעילה של המזמין להפרות של הוראות החוק והחוזה**. יצוין, כי ככל שהגדרת מטרות השימוש המותרות במידע ודרישות אבטחת המידע ברורות (כמפורט להלן), כך יקל להפעיל סעדים אפקטיביים.

3.1.3.5. במקרים המתאימים, על המזמין לדרוש **ייחוד עיסוק של הקבלן, הפרדה תאגידית בין הקבלן לגופים אחרים העוסקים במידע או הפרדה מבנית בתוך התאגיד הקבלן**, על מנת לצמצם ככל הניתן סיכון לשימוש במידע ממאגר המידע של המזמין לצרכים אחרים של הקבלן או לקוחותיו.

3.1.4. <u>אבטחת מידע ובקרה על פעילות במיקור חוץ</u>

3.1.4.1. קיום חובת אבטחת המידע חייבת להיות תנאי יסודי בכל התקשרות לצורך ביצוע שירות מיקור חוץ.

3.1.4.2. **במסגרת אפיון השירות, עוד בטרם התקשרות, על המזמין לבחון ולהגדיר את האיומים והסיכונים הנובעים מסוג המידע המועבר לקבלן, ולקבוע את אמצעי אבטחת המידע להתמודדות עימם**. ככל שרמת רגישות המידע גבוהה יותר והנזק הצפוי להיגרם לנושא המידע עם חשיפתו יהיה גדול יותר, יש ליישם אמצעי אבטחת מידע יותר קפדניים.

3.1.4.3. **בהתאם לכך על המזמין להגדיר מסמך אבטחה מחייב**, שיתייחס לכל הנושאים המפורטים ב<u>**נספח א'**</u> להנחיה זו**. מסמך זה יהיה חלק בלתי נפרד מתנאי ההתקשרות עם הקבלן, ובמקרים המתאימים אף יהיה תנאי סף להתקשרות**. לעניין זה ניתן להיעזר בת"י ISO 27001 וכן בנייר העמדה שפרסמה רמו"ט בנושא אבטחת מידע לצורך הגנת הפרטיות[4]. **בעיבוד מידע בעל רגישות גבוהה יותר, מוצע לדרוש מהקבלן עמידה בתקן האמור** או בתקן חלופי הולם.

[4] http://www.justice.gov.il/NR/rdonlyres/8D081CC2-225B-4269-95F7-BF6860654DA4/18194/tyutat_takanot_avtachat_meida_100112.pdf
במסגרת נייר העמדה יש הסדר מוצע לעניין היבטי אבטחת המידע במיקור חוץ לפיו, מסמך האבטחה, שמומלץ שיהיה חלק נפרד מחוזה ההתקשרות, יכלול הוראות לעניין נהלי סיווג והרשאה של עובדי הקבלן ומערכותיו, כללי הפרדת מערכות בין המערכות המקבלות גישה למידע, לבין מערכות אחרות בשימושו של הקבלן במהלך עסקיו, הוראות לעניין אבטחה פיזית ולוגית של המידע, הוראות לעניין מדיניות השבתה של מדיה מגנטית לרבות כוננים קשיחים וחתימה על הסכמי שמירת סודיות ע"י עובדי הקבלן.

3.1.4.4. **על המזמין לוודא הסדרה ברורה של מימוש חובת הסודיות המפורטת בסעיף 16 לחוק לגבי מורשי הגישה למידע מטעמו של הקבלן**.

3.1.4.5. **על המזמין לאסור על הקבלן להעביר לצד שלישי כלשהו מידע שקיבל במסגרת ההתקשרות, או להשתמש במידע שאליו נחשף אגב ביצוע ההתקשרות, לכל מטרה אחרת שלא קשורה ישירות לביצוע ההתקשרות**.

3.1.4.6. **יש לוודא, כי קבלן המספק שירותים למספר רב של מזמינים, מקיים את חובותיו מכוח סעיף 17א לחוק**. לעניין זה, חובה לוודא קיום הדרישה בחוק כי הקבלן יפריד את הפעילות המתבצעת עבור המזמין מפעילויות עיבוד אחרות המבוצעות על ידו.

3.1.4.7. מומלץ, כי בכל שירות מיקור חוץ ימונה ממונה אבטחת מידע כאמור בסעיף 17ב לחוק, הן אצל הקבלן והן אצל המזמין. בהתאם לקבוע בחוק, אם הקבלן משמש מחזיק עבור יותר מחמישה מזמינים, חובה עליו לקיים זאת.

3.1.4.8. על המזמין לבצע מעקב ובקרה שוטפים על קיום הוראות החוק והוראות החוזה בידי הקבלן. ככל הניתן, יש ליישם אמצעים טכנולוגיים מקובלים, כגון מערכות ניטור ובקרה, כדי לאפשר פיקוח על פעילות הקבלן ועובדיו.

3.1.4.9. על המזמין לדרוש מהקבלן דיווחים שוטפים בכל הנוגע לאופן ניהול מאגר המידע ועיבוד המידע. כמו כן, על המזמין לדרוש לקבל דיווח מידי בכל מקרה של חשש לדליפת מידע מהמאגר או שימוש החורג מההרשאה שניתנה.

3.1.4.10. על המזמין לשמור לעצמו את זכויות הפיקוח הדרושות, בהתאם לרגישות המידע וטיב פעילותו של הקבלן, לערוך ביקורות באתר הקבלן, במיוחד כשעולות תלונות נגד הקבלן או לקראת סיום ההתקשרות עמו. על המזמין לוודא כי לקבלן ברורות גם חובותיו כלפי הרשם, לרבות סמכויות הפיקוח של הרשם אצל הקבלן בהקשר של פעילות מיקור החוץ שלו עבור המזמין.

3.1.4.11. במקרים המתאימים, ובהתאם לרגישות המידע, יש לוודא כי ממונה אבטחת המידע מטעם המזמין יוסמך לבצע ביקורת, לרבות ביקורת פתע, על אופן התנהלות הקבלן בסוגיות של השימוש במידע ואבטחתו. לשם הקלה על הפיקוח, מומלץ לקבל מהקבלן הסכמה מראש כי נציגים מוסמכים של הגוף המזמין יוכלו לחדור לחומר המחשב שבשליטתו או באחזקתו, ככל הנדרש לצורכי פיקוח ובקרה על פעולותיו. אפשרות אחרת היא להסתמך על ביצוע ביקורות מסוג זה בידי צד שלישי בלתי תלוי המקובל על הקבלן והמזמין כאחד.

3.1.5. <u>זכויות נושא המידע</u> - **על המזמין לקבוע מראש הוראות ונהלים ביחס למימוש זכויות העיון והתיקון על ידי נושא המידע, כולל התייחסות לעניין זמני תגובה, עלויות**, והכל בשים לב לסעיפים 13 ו-14 לחוק ותקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), התשמ"א-1981.

3.1.6. <u>הפעלה שוטפת של שירות מיקור החוץ</u>

3.1.6.1. על המזמין לקבוע מנגנוני הטמעה והדרכה של הוראות החוזה אצל עובדי הקבלן, על מנת לוודא שעקרונות הגנת המידע האישי יופנמו בכל רובדי ארגונו של הקבלן הרלבנטיים לביצוע השירות.

3.1.6.2. יש לקבוע איש קשר מטעם הקבלן, אשר יעמוד בקשר עם מקביל לו מטעם המזמין. אנשי הקשר יתאמו ביניהם את כל הטעון בירור בקשר להדרכה והטמעה של השירות, תוך הסבר מפורש על אודות השימוש המותר במידע.

3.1.7. <u>משך שמירת המידע, ביעור המידע</u>

3.1.7.1. יש להתיר לקבלן לשמור מידע שהתקבל מהמזמין, או מידע שהקבלן צבר בעצמו אגב מתן השירות, רק למשך פרק הזמן הנדרש במישרין לביצוע תפקידו לפי החוזה.

3.1.7.2. עם סיום ההתקשרות עם הקבלן, על המזמין לוודא כי כל המידע שהגיע לקבלן במסגרת שירות מיקור החוץ נמחק מכל אמצעי המדיה שברשותו, לרבות כוננים קשיחים, אמצעי גיבוי וכל מדיה מגנטית או אופטית אחרת. ככל שקיימת הוראה בדין המחייבת שמירת המידע אצל הקבלן, יש לוודא כי אמצעי האבטחה והבקרה שהוגדרו בחוזה עם המזמין יישארו אפקטיביים לכל אורך תקופת השמירה.

3.1.7.3. ככל שנדרשת על ידי הקבלן זכות גישה למידע לאחר סיום ההתקשרות לצורך התגוננות בפני תביעות בקשר עם תפקידיו לפי החוזה, ניתן לשמור עותק של המידע באמצעי גיבוי מקובל אצל צד ג' נאמן אשר יהיה רשאי להתיר את הגישה למידע רק למטרות הנ"ל.

3.1.7.4. על המזמין לדרוש מן הקבלן תצהיר המאמת ביצוע פעולות מחיקה, ביעור והשמדה של כל המידע שהגיע אליו במסגרת ההתקשרות עמו.

3.1.8. <u>תיעוד</u> - מומלץ כי לתהליך קבלת ההחלטות לגבי כל האמור לעיל ייערך תיעוד מסודר על מנת לאפשר לרשם או לצדדים שלישים אחרים לבחון את האופן בו מתבצע מיקור החוץ.

3.2. כלי עזר ליישום האמור בהנחיה זו מצוי ב**<u>נספח ב'</u>**.

3.3. הנחיה זו אינה גורעת מהוראות חוק הגנת הפרטיות והתקנות שמכוחו, או מכוחם של חיקוקים, הוראות והנחיות רגולטורים אחרים. לעניין גופים הנתונים לפיקוח של המפקח על הבנקים בבנק ישראל או של הממונה על שוק ההון במשרד האוצר, ראו **נספח ג'**.

3.4. הנחיה זו תיכנס לתוקף ביום 19/5/12. לאחר מועד זה יפעיל רשם מאגרי מידע את מכלול הסמכויות הקבועות לו בדין על פי העמדה המפורטת בהנחיה זו.

<u>נספח א' - נושאים להתייחסות במסמך האבטחה של מזמין שירות מיקור חוץ</u>

1. אבטחה פיסית - קיום הגנה פיסית על מערכת המידע ועל התשתית שלה לרבות מבנה, אמצעי תקשורת, מסופים ותשתית חשמלית, מפני סיכונים סביבתיים ופגיעות התואמים את רגישות המידע שיעובד;
2. אבטחה לוגית - נקיטת אמצעי אבטחה הולמים, בהתאם לרמת רגישות המידע, שימנעו חדירה מכוונת או מקרית למערכת או אל קווי התקשורת בין המזמין לקבלן;
3. הפרדת מאגרי מידע - כללי הפרדת מערכות בין המערכות המקבלות גישה למידע, לבין מערכות אחרות בשימושו של הקבלן במהלך עסקיו;
4. מדיניות הוצאה משירות של מדיה מגנטית ואופטית לרבות כוננים קשיחים, אמצעי אחסון ניידים או נתיקים, מצעי גיבוי וכד';
5. נהלים - קביעת סדרי ניהול של מאגר מידע, סיווג והרשאות גישה למידע, והוראות לאיסוף, לסימון, לאימות, לעיבוד ולהפצה של המידע, בהתאם להוראות החוק והתקנות שמכוחו;
6. ניהול הרשאות:
   6.1. קביעת אופן מתן הרשאת גישה למאגר המידע והטלת הגבלות על מורשי הגישה;
   6.2. עריכת רישום מעודכן של מורשי הגישה למאגר המידע לפי הרשאות הכניסה השונות.
7. תפעול - קיום הוראות תפעול של המערכת תוך אבטחת המידע ושמירה על שלמות המידע;
8. סודיות - החתמת מורשי הגישה על התחייבות לשמירה על סודיות ועל ההוראות שנקבעו לפי הנהלים ומסמך האבטחה;
9. בקרה - קביעת סדרי בקרה לגילוי פגיעות בשלימות המידע ותיקון ליקויים.
10. קבלת עובדים – קביעת תנאים לגבי אמינות עובדים ועבר של עבירות הקשורות בשימוש במידע בהתאם לרגישות המידע.

נספח ב' - רשימת בדיקה לקיום הוראות ההנחיה בהתקשרות לשירותי מיקור חוץ

נושא	סעיף בהנחיה	תוכן הבדיקה	הערות
בדיקה ראשונית	3.1.1.1	האם רשאי וראוי להוציא את הפעילות למיקור חוץ	
	3.1.1.2	הגדרת סוג השירות והיקף המידע הנדרשים במסגרת ההתקשרות ובחירת החלופה המועדפת לאספקת השירות	
בחירת קבלן	3.1.2	בחירת הקבלן על פי עמידה בפרמטרים שונים	
תנאי התקשרות	3.1.3.1	הגדרה ברורה של מטרות שימוש מותרות על ידי הקבלן ומורשי גישה למידע מטעם הקבלן	
	3.1.3.2	וידוא של קיום חובת ההודעה מצד הקבלן לפי סעיף 11 לחוק	
	3.1.3.3	קביעת איסור על הקבלן לאיסוף או שימוש במידע לא חוקי	
	3.1.3.4	קביעת בטוחות, סעדים וכלי בקרה אפקטיביים שישמשו את המזמין בעת הפרת החוק או החוזה על ידי הקבלן	
	3.1.3.5	דרישת ייחוד עיסוק של הקבלן ו/או הפרדה תאגידית/מבנית אצל הקבלן, במקרים המתאימים	
אבטחת מידע ובקרה	3.1.4.1	קביעת חובת אבטחת המידע כתנאי יסוד להתקשרות	
	3.1.4.2	הגדרת האיומים והסיכונים הנובעים מסוג המידע המועבר לקבלן, ואמצעי אבטחת המידע להתמודדות עימם	
	3.1.4.3	הגדרת מסמך אבטחה מחייב, כחלק בלתי נפרד וכתנאי סף בהתקשרות עם הקבלן	בעיבוד מידע ברמת רגישות גבוהה, יש לחייב את הקבלן לעמוד בת"י ISO 27001
	3.1.4.4	וידוא הסדרה ברורה של מימוש חובת הסודיות על ידי מורשי גישה מטעם הקבלן	
	3.1.4.5	קביעת איסור על הקבלן להעביר מידע שקיבל בהתקשרות לצד ג' או להשתמש במידע למטרה שלא קשורה בביצוע	

נושא	סעיף בהנחיה	תוכן הבדיקה	הערות
		ההתקשרות	
	3.1.4.6	וידוא קיום חובות קבלן המספק שירותים למספר מזמינים רב מכוח סעיף 17א לחוק	במיוחד, יש לוודא כי הקבלן מפריד בין הפעילות עבור המזמין לבין פעילות עבור מזמינים אחרים או עבור עצמו
	3.1.4.7	בחינת אפשרות מינוי ממונה אבטחת מידע הן אצל הקבלן והן אצל המזמין	אצל קבלן המספק שירותים לחמישה מזמינים ומעלה זוהי חובה, לפי סעיף 17ב לחוק
	3.1.4.8	ביצוע מעקב ובקרה שוטפים אחר פעילות הקבלן לפי החוק והחוזה	רצוי לעשות שימוש גם באמצעים טכנולוגיים
	3.1.4.9	דרישת דיווחים שוטפים מהקבלן על ניהול מאגר המידע ועיבוד המידע, ודרישת דיווח מידי במקרה של חשש לדליפת מידע	
	3.1.4.10	שמירה על זכויות המזמין לבצע ביקורת באתר הקבלן ולפקח על פעילות, כולל סמכויות הפיקוח של הרשם	
	3.1.4.11	הסדרה מראש של אפשרות ממונה אבטחת המידע או צד ג' מטעם המזמין לבצע ביקורת פתע אצל הקבלן, כולל הסכמה מראש של הקבלן לחדירה על ידו לחומר מחשב	במקרים המתאימים, בהתאם לרמת רגישות המידע
זכויות נושא המידע	3.1.5	קביעה מראש של הוראות ונהלים ביחס למימוש זכויות העיון והתיקון שיוגדרו בהתאם לרמת הזיקה של הקבלן למידע	כולל התייחסות לזמני תגובה, עלויות
הפעלה שוטפת	3.1.6.1	קביעת מנגנוני הטמעה והדרכה של הוראות החוזה אצל עובדי הקבלן	
	3.1.6.2	קביעת איש קשר מטעם הקבלן ומקביל לו מטעם המזמין לתיאום הפעילות על פי החוזה	
משך שמירת המידע וביעורו	3.1.7.1	קביעת פרק הזמן המותר לקבלן לשמור את המידע	יש להגביל את פרק הזמן לתקופה הנדרשת לביצוע ההתקשרות בלבד
	3.1.7.2	וידוא מחיקת כל המידע אצל הקבלן, על כל אמצעי מדיה שברשותו	ככל שיש הוראה אחרת בדין, יש לוודא המשך קיום אמצעים האבטחה והבקרה שבחוזה

נושא	סעיף בהנחיה	תוכן הבדיקה	הערות
	3.1.7.3	העברת עותק של המידע לנאמן צד ג' לצורך התגוננות עתידית מתביעות	במידת הצורך
	3.1.7.4	קבלת תצהיר מהקבלן על ביצוע פעולות מחיקת, ביעור והשמדת כל המידע	
תיעוד	3.1.8	עריכת תיעוד מסודר של קבלת ההחלטות ביחס לביצוע מיקור חוץ שניתן יהיה להציג לרשם ולצדדים שלישיים	

נספח ג' - תחולת ההנחיה על גופים הנתונים לפיקוח של המפקח על הבנקים או של הממונה על שוק ההון

1. מטרת נספח זה היא לקבוע את אופן התחולה של ההנחיה בנושא שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי (להלן - **ההנחיה**), על רקע האמור בסעיפים 1 ו-2 להנחיה, לגבי גורמים המפוקחים על ידי המפקח על הבנקים בבנק ישראל (להלן - **המפקח על הבנקים**) ועל ידי הממונה על שוק ההון, ביטוח וחיסכון במשרד האוצר (להלן - **הממונה על שוק ההון**) (להלן ביחד - **הגורמים**).

2. לפי ידיעת הרשם, על הגורמים חלות ההוראות הבאות (להלן ביחד - **ההוראות**):

   2.1. על המפוקחים על ידי המפקח על הבנקים חלה הוראת ניהול בנקאי תקין מספר 357;

   2.2. על גופים המפוקחים על ידי הממונה על שוק ההון חלים חוזר גופים מוסדיים 6-9-2006, הוראה לניהול סיכוני אבטחת מידע של הגופים המוסדיים וחוזר גופים מוסדיים 2010-9-4, ניהול טכנולוגיות מידע בגופים מוסדיים.

3. בהתאם לכך, יראה הרשם את דרישות המינימום המפורטות בהנחיה כמתקיימות לעניין הגורמים בתנאי שבידיהם הוכחות שהם עומדים בהוראות החלות עליהם, ביישום השינויים והתוספות המפורטים להלן:

   3.1. על הגורמים לקיים את ההוראות באופן שהן חלות באופן מלא גם על מידע אישי.

   3.2. על הגורמים לקיים את ההוראות, תוך יישום קונקרטי, במסגרת דרישות ההוראות, של הנושאים הספציפיים המממשים את עקרונות החוק המפורטים בסעיפים הבאים:

      3.2.1. הוראות בעניין הגבלת מטרה, כמפורט בסעיף 3.1.3 להנחיה.

      3.2.2. הוראות בעניין זכויות נושא המידע, כמפורט בסעיף 3.1.5 להנחיה.

      3.2.3. הוראות בעניין משך שמירת המידע, כמפורט בסעיף 3.1.7 להנחיה.

   3.3. על הגורמים להתייחס באופן מתועד, במסגרת הפעלת שיקול דעת בהתאם לעקרונות ההוראות, לעקרונות הקונקרטיים המפורטים מטה:

      3.3.1. מודל שירות כפונקציה של הסיכון, כמפורט בסעיפים להנחיה.

      3.3.2. בחינת העדר חשש לניגוד עניינים של הקבלן לעניין מידע אישי כמפורט בסעיפים 3.1.2.1.3 ו- 3.1.3.5 להנחיה.

4. במקרה של ספק או אי בהירות מוצע להתייעץ עם הרשם.

מידע לגבי ההנחיה

1. **מס' ההנחיה: 2/2011**
2. **נושא ההנחיה:** שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי
3. **תאריך פרסום:** 21/11/11
4. **בתוקף מתאריך:** 19/5/12
5. **חוקים שאוזכרו**:

א. חוק הגנת הפרטיות, התשמ"א-1981.

ב. תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001.

ג. תקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), התשמ"א-1981.

6. **פסקי דין שאוזכרו**: אין.
7. **מאמרים שאוזכרו**: אין.
8. **הנחיות היועץ המשפטי לממשלה שאוזכרו**: אין.
9. **הנחיות רשם מאגרי מידע שאוזכרו**: אין.
10. **מילות מפתח:** אבטחת מידע, בעל מאגר מידע, בקרה, דליפת מידע, הדרכה, הטמעה, המפקח על הבנקים, הפרדה תאגידית, הרשאות, מזמין, מחזיק מאגר מידע, מיקור חוץ, ממונה שוק ההון, ביטוח וחסכון, מנהל מאגר מידע, ניגוד עניינים, סעדים, ערבות, קבלן, Outsourcing.
11. **עדכונים**

גרסה	פרטים	תאריך
1.1	תיקון טעות סופר בסעיפים 3.2.2 ו- 3.3.2 לנספח ג'	07.06.12